AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for detecting clones (unauthorized duplicate identities) of the client, the method comprising:

forwarding a first signal from a client to a KDC, the first signal for requesting access to a server;

verifying that the client is authorized to access the server;

transmitting an authentication token including an encrypted session key from the KDC to the client, the authentication token for providing access to the server, wherein the authentication token is valid for a time T;

receiving a second signal from an entity prior to expiration of the time T, the second signal for requesting access to the server; wherein the entity has identifying information identical to the client; and

~~if the second request is received prior to expiration of the time T, either~~ marking the entity as a possible clone or denying the second request in order to prevent access to the server.

2. (Previously Presented) The method of claim 1 wherein the encrypted session key is valid for a designated duration.

3. (Previously Presented) The method of claim 2 wherein the designated duration is for determining the time T for which the authentication token is valid.

4. (Currently Amended) A system for detecting clones of a client within a communication network, the system comprising:

a KDC;

an application server communicably coupled to the KDC;

a client for providing a first request to access the application server;

responsive to the first request, the KDC forwarding a first authentication token including an encrypted session key for accessing the application server; the first authentication token being valid for a time duration T;

the KDC receiving a second request during time T to access the application server, the second request being received from an entity having identifying information identical to the client; and

~~if the second request is received during time T,~~ the KDC denying the second request to prevent the entity from accessing the application server.

5. (Original) The system of claim 4 wherein the entity is a clone.

6. (Original) The system of claim 5 wherein the identifying information is a client identifier copied by the clone.

7. (Cancelled)

8. (Previously Presented) The system of claim 4 further comprising the client deriving a copy of the encrypted session key for accessing the application server.

9. (Previously Presented) The system of claim 8 wherein the encrypted session key is derived using a key agreement algorithm.

10. (Original) The system of claim 9 wherein the key agreement algorithm is the Diffie-Hellman algorithm.

11. (Original) The method of claim 1 further comprising using a key algorithm for authenticating communication between the KDC and the client such that all clients wishing access to the server are required to contact the KDC.

12. (Previously Presented) The system of claim 4 further comprising requiring all entities wishing to access the server to communicate with the KDC.

13 - 17. (Cancelled)

18. (Currently Amended) A system for detecting clones of a client within a communication network, the system comprising:

a KDC;

a server communicably coupled to the KDC;

a client for receiving an authentication token including an encrypted session key from the KDC, wherein the authentication token is for accessing the server, and is valid for a time duration T;

the server receiving from the client a first request to access the server, the first request being accompanied by the authentication token;

the server recording the time duration T for which the authentication token is valid;

the server receiving from an entity, a second request during the time duration T to access the server, the entity having identifying information identical to the client; and

the server either flagging or denying the second request to prevent access to the server~~, if the second request is received during the time duration T~~.

19. (Cancelled)

20. (Original) The system of claim 18 further comprising necessitating by the system, all clients wishing to access the server to communicate with the KDC.

21. (Previously Presented) The system of claim 18 wherein a ticket granting server is the server, and the ticket is a ticket granting ticket.

22. (Currently Amended) A method for detecting clones in a communication network, the method comprising:

providing an authentication token including an encrypted session key to an authorized client, the authentication token for accessing a KDC, the session key valid for a time duration T;

receiving a request during time T to access the ~~KOC~~ KDC, the request being received from an entity with the same identifying information as the authorized client; and

if the request is received during time T, flagging the entity as a possible clone or denying the request to access to the KDC.

23. (Cancelled)

24. (Original) The method of claim 1 wherein the KDC marks the entity as a possible clone or denies the second request in order to prevent access to the server.

25. (Original) The method of claim 1 wherein the server marks the entity as a possible clone or denies the second request in order to prevent access to the server.

26. (Previously Presented) The system of claim 18 wherein the KDC is the server.